00/2119
IGR 3/18J
⑧ 7ターム

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11007241 A**

(43) Date of publication of application: **12 . 01 . 99**

(51) Int. Cl **G09C 5/00**
G06F 12/14
G09C 1/00
H04N 7/08
H04N 7/081

(21) Application number: **09173168**

(22) Date of filing: **13 . 06 . 97**

(71) Applicant: **MITSUBISHI CORP**

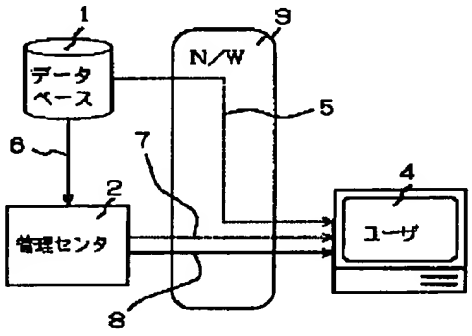
(72) Inventor: **SAITO MAKOTO**

(54) DIGITAL CONTENTS CONTROL SYSTEM USING ELECTRONIC WATERMARK

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent an unjust use on a user side device in the protection of the copy-right of digital contents by operating a use monitoring program as a process with priority higher than a digital contents control program.

SOLUTION: A data base 1 transfers ciphered digital contents to a user 4 through a network 3. Further, it transfers a cipher key for deciphering/ deciphering the ciphered digital contents to a digital contents control center 2. The control center 2 ciphers the cipher key to transmit it to the user 4. Further, the control center 2 transmits a monitoring program to the user 4. The digital contents control program incorporated in a device used by the user 4 controls the preservation/copy/transfer of the digital contents. The monitoring program interrupting into the control program detects that the preservation/copy/transfer being an irregular use are performed and embeds a visible electronic watermark in the original digital contents.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－7241

(43)公開日　平成11年(1999)１月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00	
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｇ
Ｈ０４Ｎ	7/08		Ｈ０４Ｎ	7/08	Ｚ
	7/081				

審査請求　未請求　請求項の数10　ＦＤ　（全 13 頁）

(21)出願番号　特願平9－173168

(22)出願日　平成９年(1997)６月13日

(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内２丁目６番３号

(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内

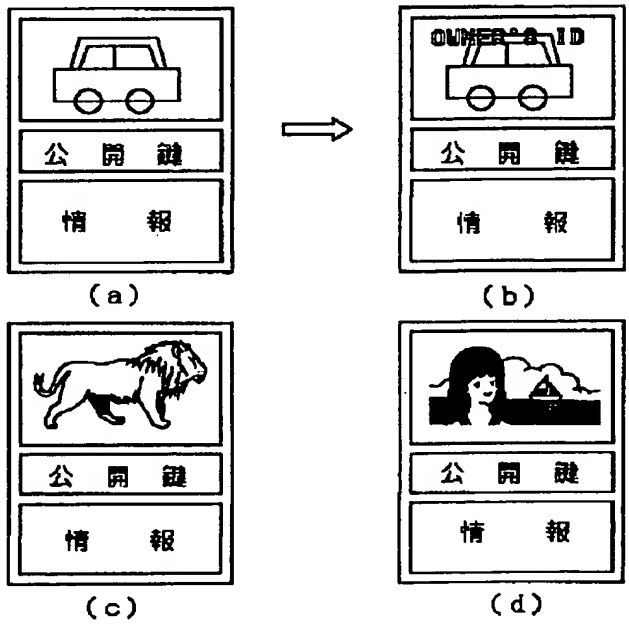
(74)代理人　弁理士　南條　眞一郎

(54)【発明の名称】　電子透かしを利用するデジタルコンテンツ管理システム

(57)【要約】

【課題】　デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの管理を行うシステム及びデジタルコンテンツの管理に使用される公開鍵を配送するシステムを提供する。

【解決手段】　デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、ネットワークあるいはデータ放送を利用して、デジタルコンテンツ管理プログラムとリンクする監視プログラムあるいは監視コマンドをユーザ装置に送信し、デジタルコンテンツの不正利用を監視する。不正利用されたデジタルコンテンツには可視透かしが埋め込まれ、以後の利用を抑制する。なお、正規の利用であっても不可視の透かしを埋め込むことにより複写・転送等の経路を確認することが可能になる。また、公開鍵を公開鍵配布画面に記入してネットワークあるいは放送により配布する。公開鍵配布画面には公開鍵所有者あるいは利用者の情報が不可視電子透かしとして埋め込まれたイメージ情報が添付されており、この電子透かしにより公開鍵あるいは利用者の正当性を確認する。



1

【特許請求の範囲】

【請求項１】　著作権主張がなされたデジタルコンテンツの管理を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
デジタルコンテンツ管理プログラムがユーザの装置のオペレーティングシステム中にマイクロカーネルとして組み込まれており；前記デジタルコンテンツ管理プログラムとリンクする利用監視プログラムが放送によって前記ユーザ装置に転送され；前記デジタルコンテンツ管理プログラムよりも割り込み優先度の高いプロセスとして前記利用監視プログラムが前記デジタルコンテンツの利用状況を監視する。

【請求項２】　前記利用状況として不正利用が検知された場合に前記デジタルコンテンツに前記ユーザの情報を可視透かしとして埋め込む、請求項１記載のデジタルコンテンツ管理システム。

【請求項３】　前記利用状況として不正利用が検知された場合に前記デジタルコンテンツに前記ユーザの情報を不可視透かしとして埋め込む、請求項１記載のデジタルコンテンツ管理システム。

【請求項４】　前記利用状況として保存・複写及び／又は転送がが検知された場合に前記デジタルコンテンツに前記ユーザの情報を不可視透かしとして埋め込む、請求項１記載のデジタルコンテンツ管理システム。

【請求項５】　公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
前記公開鍵が公開鍵配布画面に記入されて放送によって配布され；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記公開鍵の所有者の情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離して使用し；前記ユーザが前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより公開鍵所有者を確認する。

【請求項６】　前記公開鍵の所有者の情報として前記公開鍵の所有者の情報の電子指紋が利用される、請求項５記載のデジタルコンテンツ管理システム。

【請求項７】　公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
前記ユーザが前記公開鍵管理センタに前記公開鍵の配布を要求し；前記公開鍵管理センタが前記公開鍵を公開鍵配布画面に記入して前記ユーザに配布し；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記公開鍵の所有者の情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離して使用し；前記ユーザが前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより前記公開鍵の所有者を確認する。

2

【請求項８】　前記公開鍵の所有者の情報に代えて、前記公開鍵の所有者の情報の電子指紋が利用される、請求項７記載のデジタルコンテンツ管理システム。

【請求項９】　公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
前記ユーザが前記公開鍵管理センタに前記ユーザの情報を提示して前記公開鍵の配布を要求し；前記公開鍵管理センタが前記公開鍵を公開鍵配布画面に記入して前記ユーザに配布し；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記ユーザの情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離し、前記公開鍵を用いて暗号化されたデジタルコンテンツとともに前記公開鍵配布画面を前記公開鍵の所有者に転送し；前記公開鍵の所有者が前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより前記ユーザを確認する。

【請求項１０】　前記ユーザに代えて、前記ユーザの情報の電子指紋が利用される、請求項９記載のデジタルコンテンツ管理システム。

【発明の詳細な説明】

【０００１】

【利用分野】本発明は、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの著作権管理、デジタルコンテンツの秘密保護、を行うシステムに関する。

【０００２】

【従来の技術】情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム２値データであり、自然画及び動画のような情報量が格段に多いデータを取扱うことができなかった。

【０００３】ところで、各種電気信号のデジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた２値データ以外の画像信号もデジタル処理技術の開発が進められている。この画像信号のデジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をデジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【０００４】従来広く普及しているアナログコンテンツは保存，複写，加工，転送をする毎に品質が劣化するた

めに、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルコンテンツは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルコンテンツの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【０００５】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデジタルコンテンツを保存，複写，加工することによって有効活用し、加工したデジタルコンテンツを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオフラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログコンテンツである音声データ及び画像データがデジタルコンテンツ化されてデータベースとされる。

【０００６】このような状況において、データベース化されたデジタルコンテンツの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写，加工，転送等の２次利用について完成された著作権管理手段はない。なお、広告付きソフトあるいはフリーウェアと呼ばれるデジタルコンテンツは利用において原則として使用料を必要としないが、著作権は存在しており、利用の仕方によっては著作権上の制限を受ける場合がある。

【０００７】このような状況に鑑みて、本発明者はこれまでにデジタルコンテンツの著作権を保護することを目的としてこれまでに様々な提案を行ってきた。本発明者らは特開平６－４６４１９号及び特開平６－１４１００４号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平６－１３２９１６号でそのための装置を提案した。

【０００８】また、特開平７－２７１８６５号及び特開平８－１８５４４８号において、デジタルコンテンツの著作権を管理するシステムについて提案した。これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理センタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

【０００９】特開平７－２７１８６５号に記載されたシステムは、デジタル映像コンテンツのリアルタイム送信も含むデータベースシステムにおけるデジタルコンテンツの表示（音声化を含む），保存，複写，加工，転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【００１０】また、この特開平７－２７１８６５号には、デジタルコンテンツが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときにのみ復号化され、保存，コピー，転送は再び暗号化された状態で行うことが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

【００１１】本出願が関連する特開平８－２８７０１４号において著作権管理を行うためのボード，ＰＣＭＣＩＡカードあるいはＩＣカードの形態を有する復号／再暗号化用装置及び暗号鍵の寄託システムを提案した。またこの出願では著作権管理方法のテレビジョン会議及び電子商取引への応用についても言及した。

【００１２】特開平８－２７２７４５号において複数データを利用した加工データの原データ著作権及び加工データ著作権の保護を秘密鍵方式と公開鍵方式を組み合わせて加工プログラムへのデジタル署名で申込みの正当性を確認することによって行うシステムを提案した。

【００１３】特開平８－２８８９４０号において、データベース，ビデオオンデマンド（ＶＯＤ）システムあるいは電子商取引に著作権管理システムを適用するための様々の形態を提案した。

【００１４】特開平８－３２９０１１号において、複数データを利用・加工する場合の原データ及び新データの著作権保護を第三の暗号鍵及び著作権ラベルを用いて行うシステムを提案した。

【００１５】以上説明した本発明者が提案してきたデータ著作権管理システム及びデータ著作権管理装置から理解されるように、データ著作権の管理は著作権管理プログラムによって暗号化／復号化／再暗号化及び利用内容の制限を行うことによって実現される。この暗号技術及び利用制限はコンピュータを使用することによって実現される。

【００１６】さらに、ネットワークを経由して秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。伝送時の情報窃取を暗号化により防止すること

が、ＵＳＰ５５０４８１８，５５１５４４１に述べられており、その場合に複数の暗号鍵を用いることがＵＳＰ５５０４８１６，５３５３３５１，５４７５７５７及びＵＳＰ５３８１４８０に述べられており、再暗号化を行うことがＵＳＰ５４７９５１４に述べられている。

【００１７】コンピュータを効率的に使用するために、コンピュータの全体の動作を統括するオペレーティングシステム（ＯＳ）が用いられている。パーソナルコンピュータ等で使用されている従来のオペレーティングシステムはメモリ管理，タスク管理，割り込み，プロセス間通信という基本的なサービスを扱うカーネル（Kernel）と、その他のサービスを扱うオペレーティングシステムサービスで構成されていた。

【００１８】しかしながら、マイクロプロセッサの能力向上、主記憶装置として使用されるＲＡＭ価格の低下というコンピュータ側の情勢変化と、コンピュータに対する利用者からの要求性能の向上に伴い、コンピュータの全体の動作を統括するオペレーティングシステムも機能向上が要求され、以前と比較してオペレーティングシステムの規模が肥大している。

【００１９】このような肥大したオペレーティングシステムはオペレーティングシステム自身がその保存場所であるハードディスクの大きなスペースを占領するため、ユーザが必要とするアプリケーションプログラムあるいはデータを保存するスペースが不足がちになり、コンピュータの使い勝手が悪くなるという事態が発生する。

【００２０】このような事態に対処するために、最新のオペレーティングシステムはカーネルから他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステムと、セキュリティサブシステム等の中枢サブシステムとをユーザに依存する部分であるサブシステム(Sub system)として取り除き、ハードウェアの相異を吸収するＨＡＬ(Hardware abstraction Layer)，スケジューリング機能，割り込み機能，Ｉ／Ｏ管理機能等の基本的部分をマイクロカーネル(Micro kernel)とし、サブシステムとマイクロカーネルの間にシステムサービスＡＰＩ(Application Programming Interface)を介在させてオペレーティングシステムを構成している。

【００２１】このようにすることにより、機能変更あるいは追加によるオペレーティングシステムの拡張性が向上するとともに、用途に対応する移植が容易になる。また、マイクロカーネルの要素をネットワーク化された複数のコンピュータに分散配置することにより、分散オペレーティングシステムを実現することが容易になる。

【００２２】コンピュータはデスクトップ型あるいはノート型に代表されるパーソナルコンピュータ以外に、コンピュータ周辺機器、各種制御装置、通信機等に使用されている。その場合、各々の装置に適合するエンベッデッド（組み込み）用の専用オペレーティングシステムとしてマン・マシン・インターフェースが重視される汎用のパーソナルコンピュータ用オペレーティングシステムと異なり、実行の早さが重視されるリアルタイムオペレーティングシステムが採用されている。

【００２３】当然のこととして組み込まれる装置毎に異なる専用のオペレーティングシステムの開発費用は大きい。　そのため、最近ではエンベデッド（組み込み）用のリアルタイムオペレーティングシステムとしてパーソナルコンピュータ用の汎用オペレーティングシステムを転用することが提案されており、マイクロカーネルと組み合わされるサブシステムにエンベデッド用の固有のプログラムを配置することにより、組み込み用のリアルタイムオペレーティングシステムを得ることが行われている。

【００２４】オペレーティングシステムの大きな機能としてスケジューリングや割り込み処理等のタスク管理がある。タスク管理に関して、オペレーティングシステムには大きく分けて同時に１つのタスク処理しか行わないシングルタスク方式と、同時に複数のタスク処理を行うマルチタスク方式があり、マルチタスク方式はさらにタスクの切り替えが処理されるタスクに依存するマルチタスク方式と、処理されるタスクに依存しないマルチタスク方式に区分される。

【００２５】これらの中、シングルタスク方式はＭＰＵに１つのプロセスを割り当てそのプロセスが終了するまでＭＰＵを解放しないものであり、ノンプリエンプティブマルチタスク方式はＭＰＵを時分割して複数のプロセスに割り当てることができるが、実行中のプロセスがオペレーティングシステムに制御を戻さない限り他のプロセスは実行されないものであり、プリエンプティブマルチタスク方式はある時間間隔で実行中のプロセスに割り込みを行い、他のプロセスに強制的に制御を移すものである。したがって、リアルタイムのマルチタスクはプリエンプティブ方式の場合にのみ可能である。

【００２６】コンピュータにおけるタスク管理はメモリやファイルなどのシステム資源を持つ単位であるプロセスに基づいて行われ、プロセスの管理はプロセスを細分化したＣＰＵ時間を割り当てる単位であるスレッドに基づいて行われる。なお、この場合システム資源は同一プロセス内の全てのスレッドで共有され、したがって一つのプロセス中にはシステム資源を共有する一つ以上のスレッドが存在することになる。

【００２７】マルチタスク方式で処理される各タスクには優先順位(Priority Spectrum)があり、一般的には３２の段階に分けられる。この場合、割り込みを行わない通常のタスクは０－１５段階に分けられるダイナミッククラス(Dynamic Classes)に区分され、割り込みを行うタスクは１６－３１段階に分けられるリアルタイムクラス(Real-Time Classes)に区分される。割り込み処理はタイムスライスと呼ばれる割り込み可能時間（通常１０ms）を単位として行われ通常の割り込みは１０msのタイ

ムスライスで行われている。このような状況において、最近リアルタイムスライスと呼ばれる割り込み可能時間が１００μsであるタイムスライスが提案されたが、このリアルタイムスライスを利用すれば従来の１０msの割り込みよりも優先して割り込みが可能である。

【００２８】暗号技術はデータコンテンツの不正利用を不可能にするための手段であるが、その動作が完璧であるとの保証はないため、不正利用の可能性を完全に否定することができない。一方、電子透かし技術は不正利用を不可能にすることはできないが、不正利用が発見されたときには、電子透かしの内容を検証することにより不正利用であることを確定することができるが手段であり、種々の方法があるが日経エレクトロニクス６８３号，ｐ.９９～１２４に「「電子透かし」がマルチメディア時代を守る」（１９９７／２／２４，日経ＢＰ社刊）に全般的に紹介されており、また同号，ｐ.１４９～１６２,ウォルター・ベンダー他「電子透かしを支えるデータ・ハイディング技術（上）」及び６８４号,ｐ.１５５～１６８,「電子透かしを支えるデータ・ハイディング技術（下）」(IBM System Journal, vol.35, nos.3 & 4(International Business Machines Corporation)から転載）にも紹介されている。この電子透かし技術については、ＥＰ６４９０７４にも述べられている。

【００２９】

【発明の概要】本件出願においては、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの管理を行うシステム及びデジタルコンテンツの管理に使用される公開鍵を配送するシステムを提案する。

【００３０】本出願で提案するデジタルコンテンツ管理システムでは、ネットワークあるいはデータ放送を利用して著作権主張がされたデジタルコンテンツの不正利用を監視する。デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、著作権主張がされたデジタルコンテンツの利用はこのデジタルコンテンツ管理プログラムによって管理される。

【００３１】ユーザ装置は、利用監視プログラムとリンクするデジタルコンテンツ管理プログラムの管理下に置かれ、利用監視プログラムはデジタルコンテンツ管理プログラムよりも割り込み優先度の高いプロセスとして動作する。この利用監視プログラムは著作権主張がされたデジタルコンテンツの不正利用を監視し、不正利用が行われている場合には、利用の停止、警告あるいはデジタルコンテンツへの可視電子透かしの埋め込みを行う。また、正規利用の場合にも利用状況の追跡を行うために可視電子透かしに代えて不可視電子透かしを埋め込むことができる。

【００３２】さらに、本出願では公開鍵をネットワークあるいは放送により配布するシステムを提案する。公開鍵は公開鍵配布画面に記入されて配布されるが、公開鍵配布画面には公開鍵所有者の情報が不可視電子透かしとして埋め込まれたイメージ情報が添付されている。利用者が公開鍵配布画面を公開鍵管理センタに提示すると公開鍵管理センタが不可視電子透かしにより公開鍵所有者の正当性を確認する。

【００３３】公開鍵をネットワークにより配布する場合には、公開鍵所有者の情報あるいは公開鍵を請求したユーザの情報を不可視電子透かしとして埋め込み、埋め込まれた不可視電子透かしを確認することにより、公開鍵の正当性あるいはユーザの正当性を確認することができる。その場合、ユーザの情報としてユーザの公開鍵の電子指紋を利用すれば、確認が容易になる。

【００３４】

【実施例】図面を用いて本願発明の実施例を説明する。デジタルコンテンツの著作権保護においてはユーザ側装置での不正利用を如何に防止するかが最大の課題であり、特開平７－２７１８６５号の「データベース著作権管理方法」ではこれを目的としてデジタルコンテンツ管理プログラムにより復号／再暗号及び利用制限が行われる。しかしながら、著作権保護の対象であるデジタルコンテンツはユーザ側装置によって復号／再暗号が行われるため、復号／再暗号の処理及びそのために使用される暗号鍵の管理が万全であることは期しがたく、デジタルコンテンツ管理プログラムを無効化することによりデジタルコンテンツが不正に保存・複写・転送・加工される可能性がある。

【００３５】このような不正利用を制限するためには、デジタルコンテンツの復号／再暗号処理及び暗号鍵の管理を行うデジタルコンテンツ管理プログラムがユーザによって改変されないようにする必要があり、そのためにはデジタルコンテンツ管理プログラムのハードウェア（ファームウェア）化が最も確実な方法である。例えば、現在アナログテレビジョン放送においてスクランブルされた放送番組のデスクランブルに使用されている専用のスクランブルデコーダのような専用のデジタルコンテンツ管理装置を使用することによってのみデジタルコンテンツの復号／再暗号処理及び暗号鍵の管理が可能なようにする構成がある。

【００３６】このような構成は確実ではあるがシステム構成が柔軟性に欠けており、ユーザ側装置の変更あるいはデジタルコンテンツ管理プログラムの変更が行われた場合に、ユーザがこれらの変更に対応することは大変である。

【００３７】ユーザ側装置の変更あるいはデジタルコンテンツ管理プログラムの変更が行われた場合であっても、柔軟に対処するためにはデジタルコンテンツ管理プログラムがソフトウェアであることが望ましいが、デジタルコンテンツ管理プログラムがアプリケーションプログラムである場合には改変が行われる可能性がある。したがって、デジタルコンテンツ管理プログラムがソフト

ウェアであるためには、ユーザが改変を行うことができないオペレーティングシステム（ＯＳ）の固定領域であるカーネルにデジタルコンテンツ管理プログラムを組み込む必要がある。

【００３８】しかし、カーネルという固定領域にデジタルコンテンツ管理プログラムを組み込んだ場合には、データベースによってデジタルコンテンツ管理システム及び暗号システムが異なっているような場合に現実的ではない。

【００３９】前に述べたように、リアルタイムオペレーティングシステムにはカーネル領域も含む他のオペレーティングシステム内のシステムのタイムスライス時間よりも１～２桁早いリアルタイムスライス時間で割り込み動作可能なものがあり、この技術を利用することにより、全体の動作に影響を与えることなく著作権主張のあるデジタルコンテンツの利用状況を監視し、不正利用が発見された場合には、警告あるいは利用の強制中止をすることができる。次にリアルタイムオペレーティングシステムを利用してデジタルコンテンツ管理プログラムを補強する方法を説明する。

【００４０】デジタルコンテンツの不正利用は復号されたデジタルコンテンツの無許可加工、無許可保存、無許可複写あるいは無許可転送することによって行われるから、不正利用の有無は復号化デジタルコンテンツの加工、保存、複写あるいは転送の有無によって検出することができる。そのために、不正利用を監視するプロセスは、ある時間間隔でデジタルコンテンツ管理プログラムが実行中のプロセスに割り込みを行い、強制的に監視を行うプリエンプティブ方式のマルチタスクにより割り込みを行う。

【００４１】通常使用されるマルチタスクタイムスライスは１０ｍｓであり、復号／再暗号プロセスもこの時間単位で行われる。一方、最速のリアルタイムスライスは１／１００の１００μｓである。したがって、復号されたデジタルコンテンツが加工、保存、複写あるいはアップロードされているか否かを割り込み優先順位の高い監視タスクにより監視することにより、ユーザが行っている正当な利用に影響を与えることなく著作権主張のあるデジタルコンテンツの利用状況を監視することができ、不正利用が発見された場合には、警告あるいは利用の強制中止をすることができる。

【００４２】このような監視機能を有するデジタルコンテンツ管理プログラムはオペレーティングシステムのカーネル部分ではなくユーザモードで動作するサブシステム領域に組み込み、監視プロセスは優先順位の高いプロセスとする。

【００４３】この構成により、復号／再暗号によるデジタルコンテンツの利用と許可外の不正利用の有無の監視を同時に、かつ円滑に実行することができる。

【００４４】図１に、デジタルコンテンツ管理プログラムが組み込まれたオペレーティングシステムの構成を示す。このオペレーティングシステムはユーザが操作することができないカーネルモードで動作する管理部(Executive)と、ユーザが操作することができるユーザモードで動作するサブシステムからなり、管理部とサブシステムとはシステムサービスＡＰＩ(Application Programming Interface)によってインターフェースされており、ハードウェアとカーネル部の間にはＨＡＬ(Hardware abstraction Layer)が介在している。

【００４５】サブシステムは、他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステム及びセキュリティサブシステム等の中枢サブシステムとアプリケーションプログラムから構成されている。

【００４６】管理部には、マイクロカーネル(micro kernel)である仮想記憶管理機能(virtual memory manager)、オブジェクトマネージャ、ＬＰＣ(Local Procedure Call)機能、プロセスマネージャ、セキュリティ参照モニタと、最も基本的な要素であるカーネルとディスク及びネットワークとの間の入出力を管理するＩ／Ｏ管理機能(I/O manager)に、さらに著作権主張がされたデジタルコンテンツの管理を行うデジタルコンテンツ管理プログラム、すなわちデジタルコンテンツ管理機能(digital content manager)が組み込まれており、デジタルコンテンツの管理における重要な部分である保存、複写あるいは転送の管理はデジタルコンテンツ管理機能がＩ／Ｏ管理機能を管理することによって行われる。

【００４７】図２に示されたのは、本願発明が適用されるデジタルコンテンツ管理システムの実施例である。このデジタルコンテンツ管理システムにおいて、ユーザによるデジタルコンテンツ利用状況の監視はネットワークを介して行われる。この図において、１はデータベース、２はデジタルコンテンツ管理センタ、４はユーザであり、ユーザ４とデータベース１及びデジタルコンテンツ管理センタ２は公衆通信回線あるいは双方向性ＣＡＴＶ回線であるネットワーク３で接続されている。

【００４８】データベース１にはデジタルコンテンツが蓄積されており、破線で示された経路５を経由して暗号化デジタルコンテンツがユーザ４に転送される。データベース１は暗号化デジタルコンテンツを復号／再暗号するための復号用暗号鍵及び再暗号用暗号鍵を経路６によりデジタルコンテンツ管理センタ２に転送し、デジタルコンテンツ管理センタ２は転送された復号用暗号鍵及び再暗号用暗号鍵を暗号化し、破線７で示された経路を経由してユーザ４に配送する。また、デジタルコンテンツ管理センタ２は監視プログラムを実線で示された経路８でユーザ４に送信する。

【００４９】利用許可内容はユーザ４が使用する装置に組み込まれているデジタルコンテンツ管理プログラムによって管理されているが、悪意のあるユーザによってデ

ジタルコンテンツ管理プログラムが管理している範囲外の利用が行われる可能性を完全には否定することができない。デジタルコンテンツ管理プログラムはユーザ４の装置の入出力を管理しており、ユーザにおけるメモリからの入出力すなわち保存・複写・転送はすべてデジタルコンテンツ管理プログラムによって管理されており、デジタルコンテンツが保存・複写・転送されるときには再暗号化される。しかし、悪意のあるユーザによって、万一、この管理ができないようにされた場合でもデジタルコンテンツの保存・複写・転送が行われていることはデジタルコンテンツ管理プログラムに割り込む監視プログラムによって検知される。

【００５０】監視プログラムはユーザ４が使用する装置に組み込まれているデジタルコンテンツ管理プログラムとリンクしてデジタルコンテンツ管理プログラムの処理に割り込むことにより監視動作を行い、ユーザが利用許可内容を越えた利用を行なっているかどうかを監視し、このような不正規の利用である保存・複写・転送が行われていることを検知した監視プログラムは特開平７－２７１８６５号に示された警告の表示に代えて、復号処理の停止，ユーザが関知しない暗号鍵による強制再暗号化あるいは図３（ａ）に示された原デジタルコンテンツへの図３（ｂ）に示された可視電子透かしの埋め込み、あるいは図４（ｂ）に示された不可視電子透かしのデジタルコンテンツへの埋め込みを行う。

【００５１】ここで利用許可内容というのは、デジタルコンテンツの，単純利用，内蔵記憶装置への保存，外部媒体への複写，ネットワークを経由しての他の利用者への転送を指す。なお、可視電子透かしとして埋め込まれるのはユーザの名前等識別容易なものが適切である。

【００５２】ユーザ装置に内蔵されているデジタルコンテンツ管理プログラムの動作中は監視プログラムが協働している。言い換えれば、監視プログラムと協働していなければデジタルコンテンツ管理プログラムが動作しないようにされている。そのためには、ネットワークを経由して監視プログラムが起動していることをデジタルコンテンツ管理プログラムを起動させるための条件にするか、あるいはデジタルコンテンツ管理プログラムを起動させると自動的にネットワークを経由して監視プログラムが起動されるようにされている。ユーザがネットワーク経由でユーザに転送されるデジタルコンテンツを利用する場合には、転送されるデジタルコンテンツに混入して監視プログラムも転送される。

【００５３】なお、監視プログラムをデジタルコンテンツ管理プログラムに一体化し、デジタルコンテンツ管理プログラムに監視動作を行わせる監視コマンドを送信してデジタルコンテンツ管理プログラムに監視動作を行わせるようにすることもできる。

【００５４】ネットワークを介して行うデジタルコンテンツ管理システムにおいて、画像データ等情報量の多いデジタルコンテンツを扱う場合には、通信回線としてＩＳＤＮ(Integrated System for Digital Network)回線を使用することが多い。このＩＳＤＮ回線として一般的に使用されているものは、Ｂチャンネルと呼ばれるデータ伝送速度が６４Kbpsであるデータチャンネルが２チャンネル、Ｄチャンネルと呼ばれるデータ伝送速度が１６Kbpsである制御チャンネルが１チャンネルあり、当然のこととしてデジタルコンテンツは１～２チャンネルのデータチャンネルで伝送されるが、Ｄチャンネルは使用されていないことが多い。そこで、監視プログラムによる割り込み監視をこのＤチャンネルで行うことにようにすれば、デジタルコンテンツの使用に全く影響与えることなく、利用状況の遠隔監視を行うことが可能になる。

【００５５】また、公衆通信回線を使用する場合にはダウンロード用に最大５６Ｋｂｐｓのデータ伝送速度を実現することができるＡＤＳＬ(asymmetric digital subscriber line)技術を利用することにより、監視プログラムによる割り込み監視を効率的に行うことができる。

【００５６】図４に示すのは、利用許可内容に含まれている正規の保存・複写・転送の場合であっても電子透かしを埋め込む例である。この場合の電子透かしは、電子透かし検出手段によって（ｂ）のように検出される不可視電子透かしであって、電子透かし検出手段によらない場合は（ａ）に示されたように原デジタルコンテンツと一見代わりはない。なお、可視電子透かしの場合と同様に埋め込まれるのはユーザの名前等識別容易なものが適切である。

【００５７】このようにすることにより、初めは正規利用であっても後で不正利用が行われた場合に保存・複写・転送の経路を確認することができる。また、正規のものであっても保存・複写・転送が繰り返されることにより、（ｃ）に示されたように不可視電子透かしが増え、その結果デジタルコンテンツの品質が低下する。このようなことによって無限に保存・複写・転送が繰り返されることがなくなり、デジタルコンテンツの管理が容易になる。

【００５８】デジタルコンテンツ管理のために重要な要素である「再暗号化」はユーザの装置にとってかなり負担の重いプロセスである。そのため、簡易型として電子透かしを埋め込むだけでもデジタルコンテンツの不正利用を防止するには有効である。

【００５９】デジタルコンテンツの利用が有料で行われる場合に、特開平７－２７１８６５号に示されているようにユーザが予め利用許可鍵を入手するようにすれば、課金は容易に行われるが、デジタルコンテンツ管理センタが利用実績であるメータリングデータを後でポーリングによって回収して課金を行う場合には、ポーリングが行われるまでメータリングデータはユーザの管理下におかれる。そのため、悪意あるユーザによってメータリングデータの改竄が行われ、正常な課金が妨げられること

が考えられる。

【００６０】この実施例のデジタルコンテンツ管理システムにおいてはユーザがデジタルコンテンツを利用している時にはユーザ装置は常に管理センタに接続され、監視プログラムによる利用状況の監視が行われている。したがって、この監視動作の中でメータリングデータをデジタルコンテンツ管理センタに保管することにより、ポーリングの必要がなくなり、ユーザによるメータリングデータの改竄を防止することができる。また、デジタルコンテンツの利用が無料で行われる場合であっても、ユーザによる利用状況を容易に把握することができる。

【００６１】図５に示されたのは、本願発明が適用されるデジタルコンテンツ管理システムの他の実施例の構成図である。このデジタルコンテンツ管理システムにおいて、デジタルコンテンツ利用状況の監視は放送によって行われる。この図において、１１はデータベース、１２はデジタルコンテンツ管理センタ、１４はユーザであり、ユーザ１４とデータベース１及びデジタルコンテンツ管理センタ１２は公衆通信回線あるいは双方向性ＣＡＴＶ回線であるネットワーク１３で接続されている。

【００６２】データベース１１にはデジタルコンテンツが蓄積されており、破線で示された経路１５を経由して暗号化デジタルコンテンツがユーザ１４に転送される。デジタルコンテンツ管理センタ１２は暗号化デジタルコンテンツを復号／再暗号するための復号用暗号鍵及び再暗号用暗号鍵を暗号化し、破線１７で示された経路を経由してユーザ１４に配送する。また、デジタルコンテンツ管理センタ１２は監視コマンドを放送局１９に転送し、放送局１９は転送された監視コマンドを実線で示された経路１８でユーザ１４に送信する。

【００６３】この経路１８は放送電波が最も一般的であるが、有線放送であるＣＡＴＶケーブルも利用可能であり、さらにインターネット放送が行われている場合にはネットワークを利用することも可能である。

【００６４】この監視コマンドはユーザ１４が使用する装置に組み込まれているデジタルコンテンツ管理プログラムが行っている動作に割り込み、ユーザが利用許可内容を越えた利用を行なっているかどうかをデジタルコンテンツ管理プログラムに監視させ、保存・複写・転送が行われるときには復号処理を停止させ、あるいは図３に示された可視電子透かし又は図４に示された不可視電子透かしをデジタルコンテンツに埋め込む。

【００６５】ユーザ装置に内蔵されているデジタルコンテンツ管理プログラムの動作中は監視コマンドが割り込み動作を行っている。言い換えれば、監視コマンドが放送されている放送波を受信していなければデジタルコンテンツ管理プログラムが動作しないようにされている。そのためには、放送波を経由して監視コマンドを受信していることをデジタルコンテンツ管理プログラムを起動させるための条件にするか、あるいはデジタルコンテンツ管理プログラムを起動させると自動的に放送波を経由する監視コマンドを受信する。ユーザがデータ放送等でユーザに転送されるデジタルコンテンツを利用する場合には、転送されるデジタルコンテンツに混入して監視コマンドも転送される。

【００６６】デジタルコンテンツ管理プログラムはユーザ１４の装置の入出力を管理しており、ユーザにおけるメモリからの入出力すなわち保存・複写・転送はすべてデジタルコンテンツ管理プログラムによって管理され、デジタルコンテンツが保存・複写・転送されるときには再暗号化される。悪意のあるユーザによって、万一、この管理ができないようにされた場合でもデジタルコンテンツの保存・複写・転送が行われていることはデジタルコンテンツ管理プログラムに割り込む監視プログラムによって検知される。

【００６７】このような不正規の利用が行われていることを検知した監視プログラムは特開平７－２７１８６５号に示された警告の表示に代えて、図３（ｂ）に示されたような可視電子透かしの埋め込みを行う。また、利用許可内容に含まれている正規の保存・複写・転送の場合であっても図４（ｂ）及び（ｃ）に示されたような、電子透かし検出手段によってはじめて検出される不可視電子透かしを埋め込むことも可能である。

【００６８】これらの放送あるいはネットワークを介しての監視動作は、ユーザがユーザの意志で行うのではなく、著作権主張がされたデジタルコンテンツを利用する場合にはデジタルコンテンツ管理プログラムにより自動的に行われる。さらにこの動作を確実にするには、放送あるいはネットワークを介しての監視動作が行われていない場合にはデジタルコンテンツ管理プログラムによる復号／暗号化等の動作が行われないようにされる。また、著作権主張がされたデジタルコンテンツを利用する場合には監視プログラムを放送する電波の受信あるいは監視プログラムを送信する管理センタに自動的に接続される。

【００６９】次に、公開鍵の配布を行う実施例を説明する。共通鍵(common key)システムとも呼ばれる秘密鍵(secret key)システムで使用される暗号鍵の大きさは大きいものでも１００ビット程度であるのに対して、公開鍵(public key)システムで使用される暗号鍵は大きいものは１０００ビットを越す。公開鍵システムは安全性が高い反面暗号化／復号化に手間がかかるため、秘密鍵の送付、デジタル署名、認証等容量の小さいデータの暗号化に用いられ、デジタルコンテンツの暗号化は秘密鍵を用いて行われる。公開鍵システムでは公開鍵と専用鍵(private key)が組み合わされて使用され、専用鍵は所有者の管理下におかれ、他人が知ることはできないが、公開鍵はその使用目的上、他人に知らされている必要がある。

【００７０】そのために、公開鍵は種々の手段で公衆に

配布されるが、その際に所有者から直接に公開鍵を受領することができれば偽の公開鍵を配布される恐れは少ないが、そうでない場合には偽の公開鍵を受領してしまうことがある。この実施例では公開鍵を放送あるいはネットワークを経由するという間接的な配布方法においても配布された公開鍵の真偽を用にに確認することができるデジタルコンテンツ管理システム、いわば鍵配信ネットワークを提案する。

【００７１】図６に、放送により公開鍵の配布を行うデジタルコンテンツ管理システムの本発明の実施例を示す。このデジタルコンテンツ管理システムでは、公開鍵は広く一般に配送されるため、電子商取引等における公開鍵認証方式で採用されるＰＥＭ(Privacy Enhanced Mail)方式に代わる簡易認証方式として用いることができる。

【００７２】この図において、２１は公開鍵所有者、２２は公開鍵管理センタ、２３は放送局、２４はネットワーク、２５はユーザである。放送局２３は地上波アナログ、衛星アナログ、ＣＡＴＶアナログ、地上波デジタル、衛星デジタル、ＣＡＴＶデジタル等のテレビジョンあるいは音声放送局であり、走査線多重(Vertical Blanking Interval:VBI)、音声多重、データ混入等適宜の手段によりデータ放送が行われる。なお、この放送局としてインターネット放送局も利用可能である。ネットワーク２４は公衆通信回線あるいは双方向性ＣＡＴＶ回線であり、公開鍵管理センタ２２とユーザ２５との間はネットワーク２４で接続されており、放送局２３とユーザ２５との間は適宜な情報伝達媒体により接続される。

【００７３】このように構成されたデジタルコンテンツ管理システムにおいて、公開鍵所有者２１は所有する公開鍵と公開鍵所有者本人であることを証明する何らかのデータを公開鍵所有者識別用データとして経路２６により公開鍵管理センタ２２に転送する。ここで使用される公開鍵所有者識別用データとして、公開鍵所有者名等の情報を直接に利用されるが、その情報をＭＤ５ハッシュアルゴリズムによって１６バイトのデータに縮小した電子指紋を利用することもできる。

【００７４】公開鍵管理センタは図７（ａ）に示されたような公開鍵配布画面を用意しておき、所定の位置に公開鍵を挿入する。この画面は挿入された公開鍵を容易に分離して使用することができるようにＨＴＭＬ(Hyper Text Markup Language)形式あるいはＸＭＬ(eXtensible Markup Language)形式を使用して作成されており、その一部にはイメージデータが挿入されている。

【００７５】このイメージデータには、公開鍵所有者２１の識別用データ(OWNER'S ID) が不可視の電子透かしとして埋め込まれている。この不可視の電子透かしのアルゴリズム及び埋め込み位置は公開鍵管理センタのみが知っており、公開鍵管理センタは図７（ｂ）に示されたように電子透かしの内容を知ることができるが、その他の者が見た場合には図７（ａ）のような通常の画面であり、電子透かしの内容を知ることはできない。

【００７６】このイメージ画面として広告を掲載しておけば公開鍵配布に要する経費を広告掲載料によって賄うことができる。また、その他の部分には緊急情報・告知情報等の付加情報を掲載することができる。さらに、有効期間を設ける等の管理を行うためにタイムスタンプを付加してもよい。このイメージデータとしては写真を利用することが最適であるが、音声データが利用可能な場合には利用される音声データに電子透かしを埋め込むことも可能である。

【００７７】放送局２３は、このようにして作成された公開鍵配布画面を放送経路２８により放送する。

【００７８】放送された公開鍵配布画面をユーザ２５が受信するが、ユーザ２５が受信した公開鍵配布画面のイメージ画面に埋め込まれた電子透かしは不可視のものであるから、ユーザ２５は電子透かしの内容を知ることはできない。

【００７９】ユーザ２５は、放送された公開鍵配布画面から公開鍵を分離して各種電子商取引に使用するが、公開鍵の真偽に疑いを持った場合にはネットワーク２４による経路２９により公開鍵配布画面を公開鍵管理センタ２２に転送する。

【００８０】公開鍵管理センタ２２は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、図７（ｂ）に示されたように検出された公開鍵所有者の識別情報についてネットワーク２４による経路３０によりユーザ２５に通知する。

【００８１】このようにすることにより、他人が成りすましていたような場合にその成りすましを検出することができる。その場合、公開鍵所有者の識別情報として電子指紋を用いた場合には検証が極めて簡易になる。

【００８２】イメージ画面には、広告以外に公開鍵所有者の意向により、図７（ｃ）に示したような好みの画面、あるいは図７（ｄ）に示したように本人の写真を使用することが可能である。これらの場合は、掲載料を徴収して放送費用に充当することができる。

【００８３】なお、この実施例で埋め込まれる不可視の電子透かしは公開鍵管理センタのみが確認することができるようにされているが、確認だけはユーザができるようにすることもできる。その場合、公開鍵所有者識別情報として電子指紋を用い、ユーザが公開鍵所有者に電子指紋を確認するようにすることもできる。

【００８４】図８により、公開鍵がユーザの要求に応じて配布される本発明の他の実施例を説明する。図６に関して説明した放送により公開鍵を配布するデジタルコンテンツ管理システムは、主として電子商取引等不特定多数のユーザに公開鍵を配布する場合に有効なシステムである。これに対して、個人的なメールを送付する場合には公開鍵を配布する相手は特定少数であることが多く、

放送によって配布する必要はない。図８に示されたデジタルコンテンツ管理システムでは、公開鍵はネットワークを経由して個別に配送されるため、電子メイル等における公開鍵認証方式で採用されるＰＧＰ(Pretty Good Privacy)方式に代わる簡易認証方式として用いることができる。

【００８５】この図において、３１は公開鍵所有者、３２は公開鍵管理センタ、３３はネットワーク、３４はユーザである。ネットワーク３３は公衆通信回線あるいは双方向性ＣＡＴＶ回線であり、公開鍵所有者３１とユーザ３４との間及び公開鍵管理センタ３２とユーザ３４との間はネットワーク３３で接続されており、公開鍵所有者３１と公開鍵管理センタ３２との間は適宜な情報伝達手段により接続される。

【００８６】このように構成されたデジタルコンテンツ管理システムにおいて、公開鍵所有者３１は所有する公開鍵と公開鍵所有者識別用データとして公開鍵所有者本人であることを証明する何らかのデータをネットワーク３３を経由する経路３５により公開鍵管理センタ３２に転送する。

【００８７】公開鍵管理センタ３２は図７（ａ）に示された公開鍵配布画面の所定の位置に公開鍵を挿入するとともに公開鍵配布画面のイメージ画面に公開鍵所有者識別データを不可視電子透かしとして埋め込んで、経路３６により公開鍵所有者３１に返送する。なお、このデジタルコンテンツ管理システムにおいても使用される公開鍵所有者識別用データ及び公開鍵配布画面は、図６に示されたデジタルコンテンツ管理システムの場合と同一であるため、ここでの再度の説明は省略する。

【００８８】公開鍵所有者３１の公開鍵を入手しようとするユーザ３４はネットワーク３３を経由して経路３７により公開鍵所有者３１に公開鍵の配布を依頼し、この依頼に応じて公開鍵所有者３１はネットワーク３３を経由する経路３８により公開鍵配布画面をユーザ３４に転送する。

【００８９】ユーザ３４は転送された公開鍵配布画面から公開鍵を分離し、分離された公開鍵を用いて電子メールを暗号化し、公開鍵所有者３１に送信する。公開鍵所有者３１は、暗号化メールを所有する専用鍵を用いて復号する。

【００９０】ユーザ３４が、転送された公開鍵の真偽に疑いを持った場合には経路３９により転送された公開鍵配布画面を公開鍵管理センタ３２に転送する。公開鍵管理センタ３２は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、その結果を経路４０によりユーザ３４に通知する。このようにすることにより、他人が公開鍵所有者３１に成りすましていたような場合にその成りすましを検出することができる。

【００９１】この実施例では、公開鍵配布画面を公開鍵所有者３１がユーザ３４に直接に配布しているが、この他に公開鍵配布画面を公開鍵管理センタ３２が管理し、配布するように構成することもできる。

【００９２】図９及び図１０により、公開鍵がユーザの要求に応じて配布される本発明のさらに他の実施例を説明する。この実施例では、電子商取引用の公開鍵を取り扱う。図６に示された実施例及び図８に示された実施例では、電子透かしを用いて公開鍵所有者の検証を行っているが、図９及び図１０に示された実施例では、公開鍵使用者の検証を行う。

【００９３】図９に示されたデジタルコンテンツ管理システムにおいて、４１は公開鍵所有者、４２は公開鍵管理センタ、４３はネットワーク、４４はユーザである。ネットワーク４３は公衆通信回線あるいは双方向性ＣＡＴＶ回線であり、公開鍵所有者４１とユーザ４４との間、公開鍵所有者４１と公開鍵管理センタ４２との間、ユーザ４４と公開鍵管理センタ４２との間はネットワーク４３により各々接続される。

【００９４】このように構成されたデジタルコンテンツ管理システムにおいて、初めに公開鍵所有者４１は所有する公開鍵を経路４５により公開鍵管理センタ４２に転送し、公開鍵管理センタ４２は転送された公開鍵を保管している。公開鍵所有者４１に対して電子商取引で発注等の行為を行おうとするユーザ４４は、ユーザ４４の身元を証明する何らかのユーザ識別データをネットワーク４３を経由する経路４６により公開鍵管理センタ４２に転送する。

【００９５】公開鍵管理センタ４２は図１０（ａ）に示された公開鍵配布画面の所定の公開鍵挿入位置に公開鍵を挿入するとともに図１０（ｂ）に示されたように公開鍵配布画面のイメージ画面にユーザ４４の識別データを不可視の電子透かしとして埋め込んで、ネットワーク４３を経由する経路４７によりユーザ４４に転送する。

【００９６】ここで使用するユーザ識別用データとして、ユーザ名等の情報を直接に利用することも可能であるが、その情報をＭＤ５ハッシュアルゴリズムによって１６バイトのデータに縮小した電子指紋を利用することができる。

【００９７】公開鍵配布画面は挿入された公開鍵を容易に分離することができるようにＨＴＭＬ形式あるいはＸＭＬ形式を使用して作成されており、その一部にはイメージデータが挿入されている。このイメージデータには、ユーザ４４の識別データ(USER'S ID)が不可視の電子透かしとして埋め込まれている。この不可視の電子透かしのアルゴリズム及び埋め込み位置は公開鍵管理センタのみが知っており、公開鍵管理センタが確認する場合には図１０（ｂ）にように内容を知ることができるが、その他の者が見た場合には図１０（ａ）のような通常の画面であり、電子透かしの内容を知ることはできない。

【００９８】このイメージ画面は広告にしておけば公開

19

鍵配布に要する経費を広告料によって賄うことができる。また、その他の部分には緊急情報・告知情報等の付加情報を掲載することができる。さらに、有効期間を設ける等の管理を行うためにタイムスタンプを付加してもよい。このイメージデータは写真を利用することが最適であるが、音声データが利用可能な場合には利用される音声データに電子透かしを埋め込むことも可能である。

【００９９】ユーザ４４は転送された公開鍵配布画面から公開鍵を分離し、分離された公開鍵を用いて発注書を暗号化し、転送された公開鍵配布画面とともに公開鍵所有者４１に送信する。公開鍵所有者４１は、暗号化発注書を所有する専用鍵を用いて復号し、受注業務を行う。

【０１００】公開鍵所有者４１が発注者の真偽に疑いを持った場合には、ネットワーク４３を経由する経路４８により送信された公開鍵配布画面を公開鍵管理センタ４２に転送する。公開鍵管理センタ４２は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、その結果を経路４９により公開鍵所有者４１に通知する。このようにすることにより、ユーザ４４に他人が成りすましていたような場合に、その成りすましを検出することができる。

【０１０１】イメージ画面には、広告以外に公開鍵所有者の意向により、図１０（ｃ）に示したような好みの画面、あるいは図１０（ｄ）に示したように本人の写真を使用することが可能である。これらの場合は、掲載料を徴収して放送費用に充当することができる。

【図面の簡単な説明】

【図１】本発明で使用されるデジタルコンテンツ管理機能付きオペレーティングシステムの構成概念図。

【図２】デジタルコンテンツの不正利用監視を行う本発明のデジタルデータ管理システムの構成図。

20

【図３】本発明のデジタルデータ管理システムによる管理状態の説明図。

【図４】本発明のデジタルデータ管理システムによる他の管理状態の説明図。

【図５】　デジタルコンテンツの不正利用監視を行う本発明の他のデジタルデータ管理システムの構成図。

【図６】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明のデジタルデータ管理システムの構成図。

【図７】図６のデジタルデータ管理システムによる公開鍵を配布する方法の説明図。

【図８】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明の他のデジタルデータ管理システムの構成図。

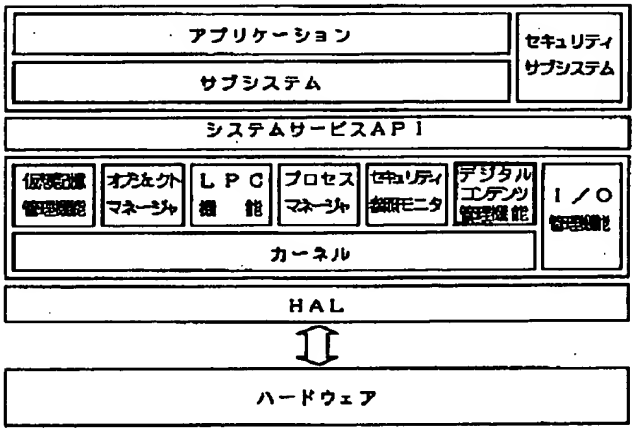
【図９】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明のさらに他のデジタルデータ管理システムの構成図。

【図１０】図９のデジタルデータ管理システムによる公開鍵を配布する方法の説明図。

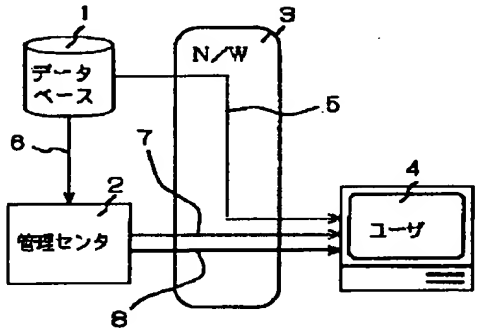
【符号の説明】

１　データベース
２　デジタルコンテンツ管理センタ
３，１３，２４，３３，４３　ネットワーク
４，１４，２５，３４，４４　ユーザ
１１　データベース
１２　デジタルコンテンツ管理センタ
１９，２３　放送局
２１，３１，４１　公開鍵所有者
２２，３２，４２　公開鍵管理センタ

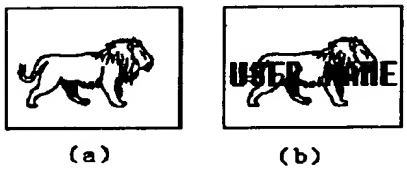
【図１】



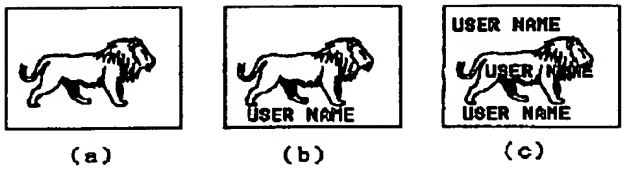
【図２】



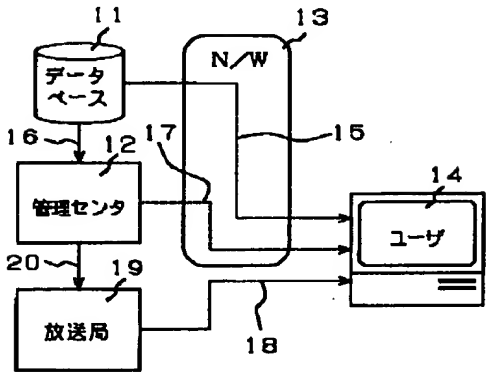
【図3】



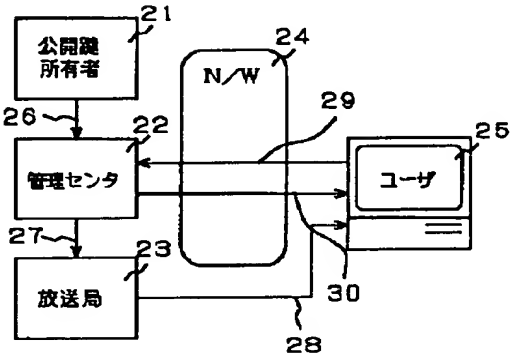
【図4】



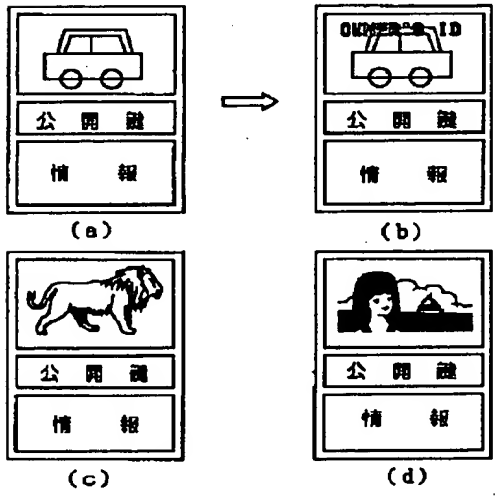
【図5】



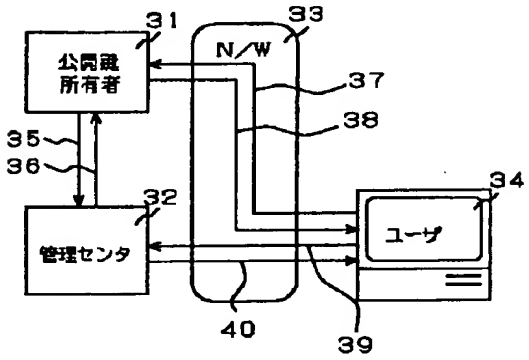
【図6】



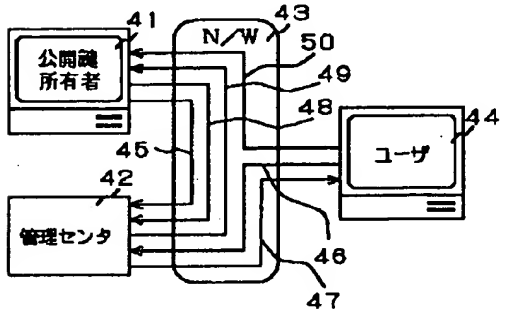
【図7】



【図8】



【図9】



【図１０】